]HackingTeam[

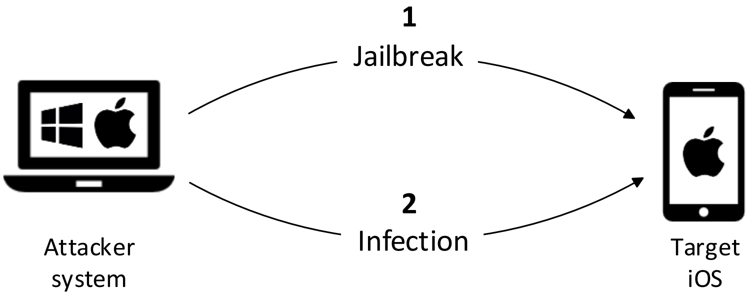
iOS Jailbreak

>>> Best Practice <<<

Apple’s iOS restricts applications that can be installed on its devices. Only those apps approved by Apple and provided through the App Store can be installed on Apple devices, such as iPhones and iPads. Jailbreaking is the process of bypassing those limitations on iOS so that applications can be installed from sources other than the App Store.

A jailbroken device can still use the App Store, iTunes and other normal functions, such as making phone calls.

This guide is intended to help you prepare the suspect’s device for RCS infection using jailbreaking.



Jailbreaking the iOS device

Jailbreaking installation requires physical custody of the device. You must also know the device password if the device has been locked by its user.

To perform the jailbreaking of an iOS device, the following software is needed:

- ✓ iTunes (https://www.apple.com/itunes/)
- ✓ iOS Jailbreak software for the appropriate iOS version:
    - iOS 7.0.x : evasi0n7 (http://evasi0n.com/)
    - iOS 7.1.x : Pangu (http://en.7.pangu.io/)
    - iOS 8.0 or 8.1 : Pangu (http://en.pangu.io/)

The following steps will allow you to jailbreak an iOS device:

Note: these operations must be performed on a Widows or OS X computer.

1. For iOS 7.0 only, edit your hosts file (where found) and add the following line:

    evasi0n.com 97.89.129.19

2. Make sure the iOS device is not password locked (unlock it, if needed)
3. Launch jailbreak software with evasi0n7 or Pangu

4. Connect the iOS device via USB
5. Click on "Jailbreak" button
6. Wait for the jailbreak process to finish the iOS device reboot

TIP - Please refer to the README file included in the Jailbreak software package for further information.

Infection Preparation

Preparing an iOS jailbroken device for RCS infection:

1. Lauch Cydia on jailbroken iOS device (Cydia is installed on the iOS device as part of the jailbreaking operation described above)
2. Tap on "Developer"
3. Search and install "**OpenSSH**" package
4. If USB infection on an iOS 7.x device is planned, search and install:
   - "**afc2add**" package
   - "**Apple File Conduit 2**" package

Optional packages you may want to consider:

Package	Description
Software Update Killer	Disables software updates that will remove the jailbreak and hide app badges. CAUTION: use of Software Update Killer can lead to detection.
adv-cmds	Support for the following commands: finger, fingerd, last, lsvfs, md, ps.
Erica Utilities	A collection of command-line utilities for various purposes.
network-cmds	Support for the following commands: arp, ifconfig, netstat, route, traceroute.
Vi IMproved	One of the best syntax highlighter.

NOTE: Restoring a device with iTunes removes the jailbreak.